STATEWIDE INFORMATION TECHNOLOGY GUIDELINE

Guidelines: Planning, Preparation, and Dealing with Information Systems Breach

Short Title: Breach Guidelines

Effective Date: February 13, 2008

Approved: Information Systems Security Project

Replaces & Supercedes: None.

I. Purpose

The purpose of these guidelines is to provide guidance to statewide entities to plan, prepare for, and manage a breach of information systems security.

II. Definitions

Refer to the Statewide Information System Policies and Standards Glossary for a list of local definitions.

Refer to the National Information Assurance (IA) Glossary, at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf for common definitions.

III. Roles and Responsibilities

These guidelines are provided in support of State of Montana law, which requires that “Department heads have overall responsibility for…security for all data…” (MCA 2-15-114)

IV. What Constitutes a Breach

There is no specific definition of what constitutes a breach. Generally, a breach is an incident wherein sensitive, confidential, protected data, or personal identifiable information is suspected of being compromised.

Determining whether a “breach” has occurred will be a judgment call made by the statewide entity’s incident response team upon evaluation of all available information.

Declaration of a “breach” may be affected by the following information attributes:

- Time-sensitivity (What may be a breach today, may not be tomorrow.)
- Legal-based (Legal requirements for protecting information.)

- Context-based (Information is sensitive when combined with other specific information, but not when combined with another type of information.)

V. Guidelines for Best Practice

A. United States Federal Trade Commission's Fair Information Principles

The Federal Trade Commission has published Fair Information Principles (http://www.ftc.gov/reports/privacy3/fairinfo.shtm) to guide organizations in the collection or storing personal information. These principles are:

- Notice/Awareness – of collection and intended use.
- Choice/Consent – provide a choice; a means of consent.
- Access/Participation – permitting personal access to a person's own information.
- Integrity/Security – use appropriate controls to secure collected information.
- Enforcement/Redress – enforce policies; provide a means of citizen redress.

These principles will not apply universally in all situations, but should be used as guidance when making collection and storage decisions.

B. Define Information as Part of an Information Management Life Cycle

Information has a life cycle, and as part of defining Information, the following properties should be declared:

- Data owner – Who's data is this?
- Data custodian – Who shall have custody of the data?
- "Notice-triggering" information – What event(s) or state of the information shall trigger notification to concerned parties?
- Assess and classify risk – What specific or general risks are associated with the information?
- Classify information – Does the information need to be classified? If so, define the classification and how will the information be marked and handled.

C. Protect Information by Implementing Information Systems Security Controls

Control guidance to protect Information includes:

- Collect minimal amount – Generally, the less information collected, the less information at risk. Business process owners should determine and specify the minimal amount of information to be collected.
- Maintain inventory – Custodians should have a current inventory available in order to advise decision-makers on what information may have been compromised by an event.
- Protect by sensitivity – Defined levels of sensitivity should be used to select levels of protection. More sensitive information should have higher levels of protection.
- Use managerial, technology, and operational controls – Best practice leverages a combination of managerial, technology, and operational controls to secure information. These should complement and not contradict each other.
- Protect high-risk environments/devices – Higher-risk environments should be provided with greater levels of security controls. Data custodians should determine and specify control solutions based upon an assessment of risk for the information.
- Train users – The risk of human factor compromise may be mitigated significantly by appropriate user training.
- Enforce policy – The organization should institute compliance practices to be conducted on a regular basis to ensure that all personnel are following policy. Corrective action should be taken as discrepancies are detected.
- Encryption – Appropriate use of encryption technology and related practices can provide ongoing protection should devices or information become lost or stolen. Business process owners should determine and specify which information should be encrypted and under what circumstances.
- Dispose of records – Records Management policies and practices should be implemented and enforced to ensure appropriate disposition of information when it is stored, archived, or destroyed.
- Define intrusion – Each organization should clearly define and communicate the events that constitute an intrusion. This allows personnel to recognize when an intrusion has occurred.
- Review Security Plan – Each organization should review their security plan - including Breach Plan component – on a regular basis;

preferably annually. The plans should be brought up-to-date if found to be inaccurate or out-of-date.

D. Prepare for Breach

Prepare for a breach by including “breach” as part of the organization Incident Response Plan. The Incident Response Plan should be developed using the guidelines provided by the National Institute for Standards and Technology (NIST) Document 800-61 Computer Security Incident Handling Guide (http://csrc.nist.gov/publications/drafts/sp800-61-rev1/Draft-SP800-61rev1.pdf)

Using the guidelines within the document ensures that the resultant plans can be aligned with federal policies, procedures and other requirements for incident response; and that full and complete guidance is considered.

Specific items to address as part of Incident Response Plan in the breach context are:

- Adopt written policies and procedures specifically addressing breach. (Use NIST 800-61 for guidance.)
- Include breach as a specific issue within the Incident Response Plan.
- Designate roles and responsibilities.
- Train employees for their specific breach-related roles and responsibilities; train users for awareness.
- Plan controls to contain, control and correct a breach.
- Require notification of data owners, and establish the parameters of how notification will occur.
- Identify law enforcement contacts. (Local and/or state/federal.)
- Consider including law enforcement recommendations in the plan.
- Document response actions. (Use the what, where, when, who, how and why framework as appropriate.)
- Review the Incident Response Plan annually for accuracy and appropriateness.

E. Notification by Including “Notification” as Part of the Incident Response Plan

Should the incident response team declare a breach event, notification may be the most important action taken. The Incident Response Plan should specifically address notification actions to be completed on event of a breach. These actions should be specified within the breach component of the Incident Response Plan, and should address:

- Detection – Acquisition of triggering information. What events/information will trigger execution of the plan?
- Timing of notification – Timely notification will be important to stakeholders affected by a breach. Timeliness of notification will depend upon attributes of the information, and defining timeframes by information classification or sensitivity in advance allows for quick notification decision at an event.
- Contact law enforcement – Notification to law enforcement may be required and governed by statute or policy. These requirements should determine notification actions in the plan.
- Whom to notify – Consider which stakeholders must be notified of a breach. These may include affected consumers/public, law enforcement, credit agencies, data owners/custodians, and the chain of command. Equally important is to determine who should not be notified. This is particularly important if an authorized investigation is in progress and notification may impede or jeopardize the investigation.
- Contact credit reporting agencies – Should a breach event potentially affect consumer credit, there may be statutory or other requirements to contact or engage the services of credit reporting agencies.
- Content of notice – Prepare notices in advance during planning, and have them pre-reviewed by legal staff and executive management. On event, content may change, but with pre-reviewed templates, the impact of last-minute changes will be minimal. Notification content should reassure rather than distress, and the recipients should be reassured that appropriate resolution actions are underway. Notification may also include other proactive actions the recipients may take to protect themselves.
- Form and style of notice – Form and style of notices should be prepared in advance based upon the anticipated audience, and the means of notification.

- Means of notification – Pre-plan primary secondary, and tertiary notification channels, such as formal letter, news bulletins, telephone contact, or email.

F. Follow-Up

After a breach has been contained and notifications completed, the organization should follow-up with a Damage Assessment and lessons-learned review. These activities should be part of the Incident Response Plan.

Follow-up by:

- Certify closure of breach – An important question that will be asked early in an event is: “Are we secure?” It is important that the organization be able to certify that indeed, the problem has been contained and resolved.
- Policy/standards implications – Are any changes needed to policies, standards, or procedures?
- Credit reporting support – Does the magnitude or nature of the breach mandate funding of a credit monitoring program? What would be the extent of the support in time and money?
- Public relations campaign – Has the organization’s reputation been impacted, and does it need specific actions to re-build the reputation?
- Lessons learned – Conduct a complete review of the event to determine:
  - What part of the plan was completed correctly?
  - What was not accomplished to standard?
  - What changes need to be incorporate into the plan or next event?

G. Changes and Exceptions

Changes and exceptions to these guidelines are governed by the Procedure: Development of Statewide Information Technology Procedures and Guidelines. Requests for a change to these guidelines are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form.

VI. Compliance Criteria

This information is provided as guidance only. Statewide entities should use this guidance in conjunction with other policies, standards and procedures as applicable.

VII. Closing

Thee guidelines may be followed unless they conflict with negotiated labor contracts or specific statutes, which shall take precedence to the extent applicable.

For questions or change requests on this policy, please e-mail ITpolicy@mt.gov.

Or, you may contact the Information Technology Services Division at:

PO Box 200113
Helena, MT 59620-0113
(406) 444-2700

VIII. Cross-Reference Guide

A. State/Federal Laws

- MCA 2-15-114
- MCA 30-14-1701, et seq.
- MCA 30-14-1704

B. IT Procedures or Guidelines Supporting These Guidelines

- Procedure: Development of Statewide Information Technology Procedures and Guidelines
- The Federal Trade Commission Fair Information Principles (http://www.ftc.gov/reports/privacy3/fairinfo.shtm)
- National Institute for Standards and Technology (NIST) Document 800-61 Computer Security Incident Handling Guide (http://csrc.nist.gov/publications/drafts/sp800-61-rev1/Draft-SP800-61rev1.pdf)

IX. Administrative Use

History Log	
Control ID:	GDE-20080213a
Approved Date:	February 13, 2008
Effective Date:	February 13, 2008
Change & Review Contact:	ITpolicy@mt.gov
Review:	Event Review: Any event affecting these guidelines may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	Five years from Effective Date
Last Review/Revision:	
Changes:	